# State of Washington Windows 2000
# Root Domain Health Monitoring Plan

| | |
|---|---|
| Project: | State of Washington Multi-Agency Forest Project |
| Title: | Root Domain Health Monitoring Plan |
| Version: | 1.0 |
| Status: | Draft for Comment |
| Date: | June 23, 2001 |

## Revision History

| Version | Date | Comments |
|---|---|---|
| 1.0 | April 30 2001 | Initial draft, outline major tasks for daily, weekly and monthly activities.<br>Sent to Dev Group for review |
| 1.1 | May 9, 2001 | Incorporate feedback from Dev Group.<br>Changed document title page, and added revision history.<br>Add screen captures.<br>Add step-by-step instructions for major activities.<br>Add Daily Activity Template. |
| 1.1 | May 11, 2001 | Merged document changes between the version of Julie Xu and Anthony Witecki.  Renamed document to not include version information. |

## Contributors

**Authors:** Julie Xu (Microsoft Consulting Services), Krishnan P Iyer (Microsoft Consulting Services), Brent McCarthy (Microsoft Consulting Services), Anthony Witecki (Microsoft Consulting Services).

**Reviewers**: Lance Calisch (DIS – State of WA), Jane Rasmussen (Microsoft Consulting Services), and other members of the Win2K development group.

**Approvers:**

**Table of Contents**

# Introduction

Health monitoring is the process of ensuring availability, reliability and capacity planning in an application or network environment. Several options are available to administrators when deciding on a health monitoring plan, including several automated tasks, services, and monitoring applications.

The purpose of this document is to outline a health plan for the root domain, using only the tools available with Windows 2000 Server. This document is intended to be a work-in-process. In other words, as new applications are purchased or discovered, the methods used to achieve the objectives in this document are subject to change.

## How to Use This Document

This document should be a guideline for health monitoring. The objectives stated in this document are the ultimate responsibility of DIS. The methods used to achieve these objectives may change over time. However, the document demonstrates some of the performance analysis possibilities available in Windows 2000.

## Root Domain Management Personnel

**Objective:** Document the members of the Root Domain Administration team.

The Windows 2000 (Win2K) forest root domain in the production environment is called WA.LCL. Responsibility for managing the root domain will be delegated to selected personnel at the Department of Information Services (DIS). Please contact the DIS Help Desk for questions, problems, and escalations.

# Hardware Performance

**Goal:** to ensure that adequate hardware resources exist in the root domain to handle the core functions of Windows 2000 Server.

## Server Build Documents

**Objective:** ensure that Windows 2000 operating system images are consistent across all domain-function servers in the root.

Server build documents are useful for ensuring that new servers introduced into the root (or existing servers being rebuilt) are prepared with a consistent image. Server build documents do not include procedures for installing Active Directory using the DCPromo application.

| **Server Build Requirements** |
|---|

| | |
|---|---|
| **Software is installed in the following order.** | 1. Windows 2000 Server. Be sure to include IIS components as part of the installation.<br>2. Windows 2000 Server Support Tools<br>3. The most recent Windows 2000 Service Pack approved by the Forest Resource Group. This should be installed with the "/S" switch to ensure that new components receive the most recent bits.<br>4. Windows 2000 Resource Kit Utilities with the most recent approved service release. |

| | |
|---|---|
| **Configuration Requirements** | 5. Windows 2000 servers must have 2 physical drives. The system partition should be mirrored and the secondary partition should be at least twice the size of the expected Active Directory database (currently 18 GB is recommended). This should be RAID-5 for reliability.<br>6. All drives must be formatted NTFS.<br>7. Configure Internet Support. Use Manual Configuration with no proxy server.<br>8. Reset the administrator password to equal ########. |

## Server Count

**Objective:** ensure that DCPromo procedures are in place for adding new domain controllers, global catalogs or FSMO servers to the root as well as replacing existing servers on new hardware.

**Response time** is the measure of time required to do work from start to finish. In the active directory environment, response time is typically measured on the domain controllers or collected by a monitoring server using the trace log feature in the Windows 2000 performance tools.

As response times degrade, it is necessary at some point to add new hardware to the root environment. New hardware will include: faster or additional processors, additional RAM, or additional servers.

### Standard Hardware Configuration

The standard hardware configuration for production servers in the root domain is as follows. The **minimum** hardware configuration for DIS Windows 2000 Servers is:

**Server Brands:** Compaq Proliant.

**Processors:** Dual Pentium IIIs, running at 750 Mhtz or greater.

**RAM:** 512 MB

**Hard Drives:** The system should be configured with 2 logical drives on two separate physical drives, to be used by the operating system and active directory for maximum disk access times. System partitions must be 9 GB and Active Directory partitions must be at least twice the size of the Active Directory Database (current recommendation is 18 GB).

### Upgrading Existing Servers

This section outlines the procedures that should be followed for making hardware changes to the Physical RAM. This will be done only on an as-needed basis.

| **To Add New Physical RAM to a Root Server** | |
|---|---|
| **Schedule a Service Time.** | 1. Notify all affected parties via email about the date, time and expected |

| | |
|---|---|
| **Time.** | outage for the server. Make it quite clear that only individual servers are affected, not the domain service.<br>2. At the appropriate time, power down the server. |
| **Install RAM and Reboot machine** | 3. Install the Physical RAM in accordance with the instructions provided by the PC manufacturer.<br>4. Power the machine back on and bring it back into the domain. Check to ensure that all critical services are running. |

### Adding New Servers

New servers should be purchased, as needed, in compliance with the Standard Hardware configuration identified above. Follow procedures outlined on Page 11 for the server build process. To promote the domain controller into the root domain, following the procedures listed in the root domain requirements document.

## Processor Utilization

**Objective:** Monitoring the processor utilization on your domain controllers will allow you to determine if your domain controllers are being overloaded by logon or replication traffic. This will also allow you to verify that you are meeting your service level agreements.

Performance counters can be monitored real time or logged over time for base lining purposes. Baseline metrics should be captured using the Performance Logs, whereas real-time metrics are captured using Performance Monitor. This exercise is intended to measure overall processor performance. Specific services available through Active Directory may encounter processor bottlenecks that are not apparent in this evaluation.

## Establishing a Processor Utilization Baseline

Begin a monitoring routine with an examination of processor usage under the normal workload. This establishes a baseline or reference point for processor usage. The baseline is generally not a single value, but a range within which processor usage can fluctuate and still provide acceptable performance. The baseline can be used to identify trends, such as increasing processor demands over time, or to recognize problems that arise from a sudden change.

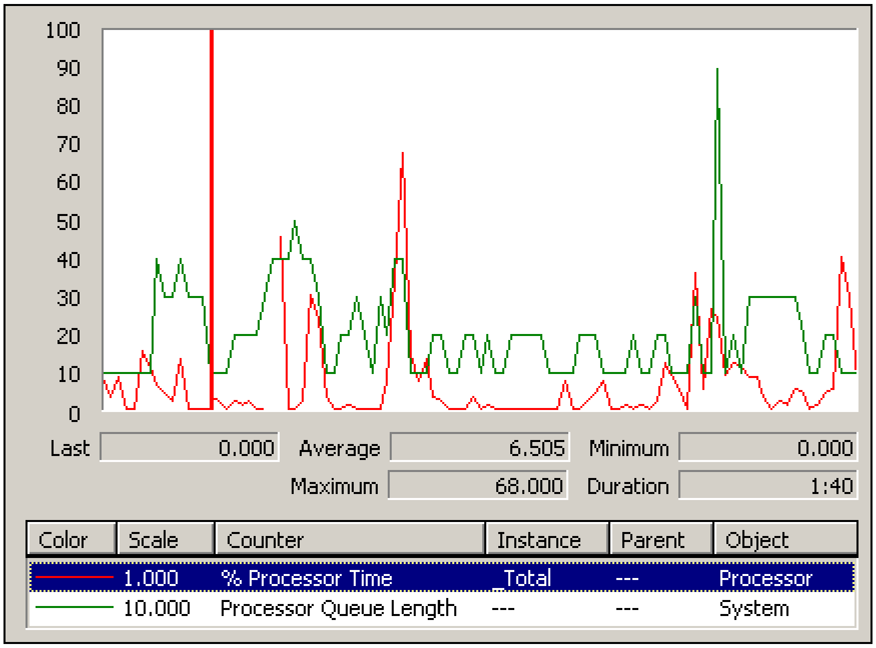
The monitoring routine will be run for a period of 7 days, running at 1 minute intervals 24 hours per day.  The routine should be re-evaluated every month or after any major change.  For trend analysis purposes, baseline logs should be kept for at least six months.

The following counters should be included in the baseline metrics for processor activity.

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| PROCESSOR | % PROCESSOR TIME | The percentage of time the processor was |

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| | | busy during the sampling interval. Across all processors, this value should be blow 85%. |
| SYSTEM | PROCESSOR QUEUE LEN | An instantaneous count of threads that are in the processor queue. If this counter has a sustained value of two or more threads, the processor might be a bottleneck. In general, it should be 0. |

When trouble is suspected, the same performance monitor counters can be viewed real time and compared against the established baseline metrics. For appearance purposes, the %Processor Time counter is scaled at 1.000 (represented as a percentage on the graph) and the Queue length is scaled at 10 times the actual count. This makes it easier for administrators to differentiate changes in values.



Last 0.000 Average 6.505 Minimum 0.000
Maximum 68.000 Duration 1:40

| Color | Scale | Counter | Instance | Parent | Object |
|---|---|---|---|---|---|
| 🟥 | 1.000 | % Processor Time | _Total | --- | Processor |
| 🟩 | 10.000 | Processor Queue Length | --- | --- | System |

**Figure 1 - Processor Counters Displayed in Real Time**

| **To set up a baseline for Processor** | |
|---|---|
| **Create a new log using Windows 2000 Performance tools.** | 1. Open the Performance Application from the Administrative Tools Folder on the Start menu.<br>2. Expand performance logs and alerts.<br>3. Right-click counter logs and select New Log Settings.<br>4. Give the new log a name, describing the type of counters and period (e.g.: Processor Baseline May 2001). |

| | |
|---|---|
| **Specify counters, intervals, and file locations.** | 5. In the General Tab, click the add button to add the counters listed in the above table.<br>6. Set the sampling rate to every five minutes.<br>7. Switch to the Log Files Tab.<br>8. Specify a location on the D drive where the log files are to be archived (D:\performanceLogs\).<br>9. Ensure that file names end with the nnnnn format (this keeps an identity value that makes troubleshooting easier).<br>10. Switch to the Schedule tab. Specify that start date as 12:00 PM (noon) for the next available Monday.<br>11. Specify the stop log for 12:00 PM (noon) exactly one week later.<br>12. Click Ok to save and schedule the performance log. |

## Memory Utilization

**Objective:** Ensure that each system in the root domain has adequate physical and virtual memory to accommodate the workload assigned to it.

Low memory conditions can slow the operation of applications and services on the server and impact the performance of other resources in the system. For example, when the computer is low on memory, *paging* — that is, the process of moving virtual memory back and forth between physical memory and the disk — can be prolonged, resulting in more work for the disks. Because it involves reading and writing to disk, this paging activity might have to compete with whatever other disk transactions are being performed, intensifying a disk bottleneck. In turn, all this work by the disk can mean the processor is used less or is doing unnecessary work, processing numerous interrupts due to repeated page faults. In the end, applications and services become less responsive.

To accomplish this objective, examine the physical memory usage under a normal workload to establish a baseline or reference point for physical memory usage. The baseline is generally not a single value but a range within which physical memory usage can fluctuate and still provide acceptable performance. You can use the baseline to identify trends, such as increasing physical memory demands over time, or to recognize problems that arise from a sudden change.

### Establishing a Memory Usage Baseline

To determine a baseline for your system, use the following counters to create logs of memory usage over a period of seven days. Re-evaluate memory usage on a monthly basis or whenever significant changes are introduced into the environment. Metrics should be taken 24 hours per day in five minute intervals.

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| MEMORY | PAGES/SEC | Indicates the number of requested pages that were not immediately available in RAM and had to be read from the disk or had to be |

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| | | written to the disk to make room in RAM for other pages. If your system experiences a high rate of hard page faults, the value for Memory\Pages/sec can be high. |
| MEMORY | AVAILABLE BYTES | Indicates how much physical memory is remaining after the working sets of running processes and the cache have been served. |
| PAGING FILE | % USAGE | Usage of the Paging file. Indicates how much disk activity is occurring to support memory functions. |

As you monitor the values of these counters, you might see occasional spikes. Typically, you can exclude these from your baseline because it is the consistent, repetitive values with which you are most concerned; the range of values that seem to appear consistently constitutes your baseline. When values fall outside of these ranges for extended periods, server activity should be investigated as more memory may be required to adequately function.

When trouble is suspected, the same performance monitor counters can be viewed real time and compare against the established baseline metrics.

| **To set up a baseline for Memory** | |
|---|---|
| **Create a new log using Windows 2000 Performance tools.** | 1. Open the Performance Application from the Administrative Tools Folder on the Start menu.<br>2. Expand performance logs and alerts.<br>3. Right-click counter logs and select New Log Settings.<br>4. Give the new log a name, describing the type of counters and period (e.g.: Memory Baseline May 2001). |

| | |
|---|---|
| **Specify counters, intervals, and file locations.** | 5. In the General Tab, click the add button to add the counters listed in the above table.<br>6. Set the sampling rate to every five minutes.<br>7. Switch to the Log Files Tab.<br>8. Specify a location on the D drive where the log files are to be archived (D:\performanceLogs\).<br>9. Ensure that file names end with the nnnnn format (this keeps an identity value that makes troubleshooting easier).<br>10. Switch to the Schedule tab. Specify that start date as 12:01 PM (noon) for the next available Monday.<br>11. Specify the stop log for 12:01 PM (noon) exactly one week later.<br>12. Click Ok to save and schedule the performance log. |

## Hard Disk Space and Performance

**Objective:** to ensure that adequate hard drive space remains for handling domain services, performance meta-data (performance log files, event logs, etc.) and system resources (paging file, etc.).

Disk-usage statistics help you balance the workload of network servers. System Monitor provides physical disk counters for troubleshooting, capacity planning, and for measuring activity on a physical volume.

**NOTE:** When testing disk performance, log performance data to another disk or computer so that it does not interfere with the disk you are testing.

Unlike processors and RAM, where the solution to a bottleneck typically involves throwing more hardware at the problem, a disk bottleneck can be overcome any of three ways:

1. If the server uses a RAID, add more disk drives, using faster drives if possible, and increase the memory cache size on the controller.
2. If the server does not use a RAID, switch to higher-speed disk drives.
3. Use Disk Defragmenter to optimize disk space.

### Establishing a Baseline for Disk Performance

To balance loads on network servers, you need to know how busy the server disk drives are.  Use the following counters when establishing your baseline.

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| PHYSICAL DISK | % DISK TIME | Indicates the percentage of time a drive is active. |
| PHYSICAL DISK | CURRENT DISK QUEUE LENGTH | Indicates how many system requests are waiting for disk access.  This value should be no higher than 2.5 times greater than the number of spindles on the physical disk. |

Most disks have one spindle, although RAID devices usually have more. A hardware RAID device appears as one physical disk in System Monitor; RAID devices created through software appear as multiple drives (instances). You can either monitor the Physical Disk counters for each physical drive (other than RAID), or you can use the _Total instance to monitor data for all the computer's drives.

Use the values of the Current Disk Queue Length and % Disk Time counters to detect bottlenecks with the disk subsystem. If Current Disk Queue Length and % Disk Time values are consistently high, consider upgrading the disk drive or defragmenting the volume.

| **To set up a baseline for Physical Disks** | |
|---|---|
| **Create a new log using Windows 2000 Performance tools.** | 1. Open the Performance Application from the Administrative Tools Folder on the Start menu.<br>2. Expand performance logs and alerts.<br>3. Right-click counter logs and select New Log Settings.<br>4. Give the new log a name, describing the type of counters and period (e.g.: Physical Disk Baseline May 2001). |
| **Specify counters, intervals, and file locations.** | 5. In the General Tab, click the add button to add the counters listed in the above table.<br>6. Set the sampling rate to every five |

| | |
|---|---|
| | minutes.<br>7. Switch to the Log Files Tab.<br>8. Specify a location on the D drive where the log files are to be archived (D:\performanceLogs\).<br>9. Ensure that file names end with the nnnnn format (this keeps an identity value that makes troubleshooting easier).<br>10. Switch to the Schedule tab.  Specify that start date as 12:02 PM (noon) for the next available Monday.<br>11. Specify the stop log for 12:02 PM (noon) exactly one week later.<br>12. Click Ok to save and schedule the performance log. |

**Reminder:** use a separate machine to evaluate disk performance, as the performance log itself utilizes the hard drive when recording results.

### Preserving Space on Hard Drives

Active Directory automatically performs online defragmentation of the database at certain intervals (by default, every 12 hours) as part of the Garbage Collection process. Online defragmentation does not reduce the size of the database file (Ntds.dit), but instead optimizes data storage in the database and reclaims space in the directory for new objects.

Performing an offline defragmentation creates a new, compacted version of the database file. Depending on how fragmented the original database file was, the new file may be considerably smaller.

Each month, DIS should examine the size of the NTDS.DIT file and determine if sufficient space exists on the hard drive. If not, or if hard drive performance appears to be suffering, DIS should implement the procedures below for doing an offline defragmentation. Please see Q232122 for more information about this process.

**Note:** This procedure requires that the Server affected be rebooted. It should only happen on one domain controller at a time, only during off-peak hours (when replication is not happening).

| **To Perform Offline Defragmentation** | |
|---|---|
| **Reboot the Server and Logon as the Local Administrator in Directory Service Restore mode.** | 1. Back up Active Directory. Windows 2000 Backup natively supports backing up Active Directory while online. This occurs automatically when you select the option to back up everything on the computer in the Backup Wizard, or independently by selecting to back |

| | |
|---|---|
| | up the "System State" in the wizard.<br>2. Reboot the domain controller, select the appropriate installation from the boot menu, and press F8 to display the Windows 2000 Advanced Options menu. Choose Directory Services Restore Mode and press ENTER. Press ENTER again to start the boot process.<br>3. Log on using the Administrator account with the password defined for the local Administrator account in the offline SAM. For more information about the use of the offline SAM database, please see the following Article in the Microsoft Knowledge Base: Q223301 Protection of the Administrator Account in the Offline SAM |

| | |
|---|---|
| **Open the NTDSUTIL application.** | 4. Click Start, point to Programs, point to Accessories, and then click Command Prompt. At the command prompt, type ntdsutil, and then press ENTER.<br>5. Type files, and then press ENTER.<br>6. Type info, and then press ENTER. This displays current information about the path and size of the Active Directory database and its log files. Note the path. |
| **Determine the new location for the compacted file.** | 7. Establish a location that has enough drive space for the compacted database to be stored.<br>8. Type compact to drive:\directory, and then press ENTER, where drive and directory is the path to the location you established in the |

| | |
|---|---|
| | previous step. NOTE: You must specify a directory path. If the path contains any spaces, the entire path must be surrounded by quotation marks (for example: Compact to "c:\new folder"<br>9. A new database named Ntds.dit is created in the path you specified.<br>10. Type quit, and then press ENTER. Type quit again returning to the command prompt.<br>11. Copy the new Ntds.dit file over the old Ntds.dit file in the current Active Directory database path you noted in step 6.<br>12. Restart the computer normally. |

# Service: DNS

**Goal:** to ensure that the DNS services provided by the root domain meet the needs of the agency customers for name resolution.

## DNS Performance

**Objective:** to ensure that proper hardware and network resources exist to allow DNS activity to occur in a timely manner.

DNS Servers in the root domain are primarily responsible for handling the following tasks:

1. Secure Dynamic Updates
2. DNS Queries for Hosts and Services

Additionally, we are interested in how DNS affects overall server performance, so we will want to monitor some of the DNS Server Memory counters.

Since the Active Directory enabled zones are configured to accept only secure dynamic updates, the update rate (update requests per second) can decrease. Network performance might also be a factor in these cases since the directory database may require network activity to process updates.

### Establishing a DNS Baseline

To accomplish the performance objective for DNS Services, it is necessary to establish a baseline of metrics for updates, queries, and memory usage.  This information will be captured using the Performance monitor tool in Windows 2000 and should be captured during "normal activity" over a period of 7 days.  It should be recorded in 1 minute intervals 24 hours per day.  The baseline will need to be re-evaluated for each significant change to the environment (new agencies, etc.).  The following counters will be used.

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| DNS | Caching Memory | The total amount of system memory in use by |

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| | | the DNS Server service for caching. |
| DNS | Record Flow Memory | The total amount of system memory in use by the DNS Server service for record flow. |
| DNS | Secure Update Received Per Second | The average number of secure update requests received by the DNS server in each second. |
| DNS | TCP Query Received Per Second | The total number of TCP queries received by the DNS server. |
| DNS | TCP Response Sent Per Second | The total number of TCP responses sent by the DNS server. |

As you monitor the values of these counters, you might see occasional spikes. Typically, you can exclude these from your baseline because it is the consistent, repetitive values with which you are most concerned; the range of values that seem to appear consistently constitutes your baseline. When values fall outside of these ranges for extended periods, server activity should be investigated.

When trouble is suspected, the same performance monitor counters can be viewed real time and compare against the established baseline metrics.

| **To set up a baseline for DNS** | |
|---|---|
| **Create a new log using Windows 2000 Performance tools.** | 1. Open the Performance Application from the Administrative Tools Folder on the Start menu.<br>2. Expand performance logs and alerts.<br>3. Right-click counter logs and select New Log Settings.<br>4. Give the new log a name, describing the type of counters and period (e.g.: DNS Baseline May 2001). |
| **Specify counters, intervals, and file locations.** | 5. In the General Tab, click the add button to add the counters listed in the above table. |

| | |
|---|---|
| | 6. Set the sampling rate to every five minutes.<br>7. Switch to the Log Files Tab.<br>8. Specify a location on the D drive where the log files are to be archived (D:\performanceLogs\).<br>9. Ensure that file names end with the nnnnn format (this keeps an identity value that makes troubleshooting easier).<br>10. Switch to the Schedule tab. Specify that start date as 12:00 PM (noon) for the next available Monday.<br>11. Specify the stop log for 12:00 PM (noon) exactly one week later.<br>12. Click Ok to save and schedule the performance log. |

## DNS Completeness

**Objective:** to ensure that all agency name servers exist in the root configuration and that zone transfers and complete and run without incident.

### Validation of DNS Name Server Records in the Root

On a monthly basis, or during times of troubleshooting, it is necessary to verify that resource records exist for each of the child domain name servers. This ensures proper zone delegation and active directory replication. You will need to compare the entries listed in the DNS service pane with the authoritative list maintained by DIS for valid name servers. During this check, you should also pay attention to resource records that are not supposed to be included.

| **To validate Resource Records in DNS** | |
|---|---|
| **Open DNS Administrator** | 1. Select DNS from the Administrative Tools folder on the start menu. |

| | |
|---|---|
| **console in MMC.** | 2. Resource Records of interest are Host Records (indicated by an "A") and Name Server Records (indicated by a "NS"). |

### Monitoring DNS Events in the Windows 2000 Event Log

As part of the daily monitoring of Active Directory health, the system and DNS Server logs should be checked for the following events. To view event logs, open the event viewer from the administrative tools folder in the start menu.

| NBR | EVENT LOG | DESCRIPTION |
|---|---|---|

| NBR | EVENT LOG | DESCRIPTION |
|---|---|---|
| 4011 | DNS SERVER | The DNS server was unable to add or write an update of domain name _ldap in zone to the Active Directory.<br>When a Windows 2000-based Active Directory-integrated DNS server that hosts a global catalog boots, the registration of specific SRV records may not succeed. The service startup order prevents certain SRV records from being registered because those services start before DNS is ready to receive registrations on a global catalog server.<br>To work around this behavior, specify a different Windows 2000-based Active Directory-integrated DNS server on the DNS tab in the Advanced TCP/IP Settings dialog box.<br>See Q252695 for more information. |
| 4015 | DNS SERVER | The DNS server has encountered a critical error from the Active Directory. Check that the Active Directory is functioning properly.<br>See Q267855 for more information. |

| NBR | EVENT LOG | DESCRIPTION |
|---|---|---|
| 7062 | DNS SERVER | The DNS server encountered a packet addressed to itself.<br>Make sure that there is no lame delegation for this server. A lame delegation occurs when one server delegates a zone to a server that is not authoritative for the zone.<br>Check the forwarders list to make sure that it does not list itself as a forwarder.<br>If this server includes secondary zones, make sure that it does not list itself as a master server for those zones.<br>If this server includes primary zones, make sure that it does not list itself in the notify list. |
| 5781 | SYSTEM | Dynamic registration or deregistration of one or more DNS records failed because no DNS servers are available. See Q252695 for more information. |

## DNS Troubleshooting (Advanced Logging)

The DNS log is a special troubleshooting tool that can be optionally configured if you believe specific problems are occurring with the DNS Server. Typically, these procedures should only be used during the implementation of a troubleshooting plan to locate specific problems. You can configure the DNS server to create a log file that records the following types of events:

1. Queries
2. Notification messages from other servers
3. Dynamic updates
4. Content of the question section for DNS query message
5. Content of the answer section for DNS query messages
6. Number of queries this server sends
7. Number of queries this server has received
8. Number of DNS requests received over a UDP port
9. Number of DNS requests received over a TCP port
10. Number of full packets sent by the server
11. Number of packets written through by the server and back to the zone

The DNS log appears in % SystemRoot%\System32\dns\Dns.log. Because the log is in RTF format, you must use WordPad to view it. You can change the directory and file name in which the DNS log appears by adding the following entry to the registry with the REG_SZ data type:

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters \LogFilePath**

Set the value of LogFilePath equal to the file path and file name where you want to locate the DNS log. By default, the maximum file size of Dns.log is 4 MB. If you want to change the size, add the following entry to the registry with the REG_DWORD data type:

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters \LogFileMaxSize**

Set the value of LogFileMaxSize equal to the desired file size in bytes. The minimum size is 64 Kb. Once the log file reaches the maximum size, Windows 2000 writes over the beginning of the file. If you make the value higher, data persists for a longer time, but the log file consumes more disk space. If you make the value smaller, the log file uses less disk space, but the data persists for a shorter time.

| **To configure the server to log DNS Events** | |
|---|---|
| **Select logging options from DNS console.** | 1. In the DNS console, click the box next to the server, right-click the server, and then click Properties.<br>2. Click the Logging tab, and then select the options you want to log.<br>3. Available logging option are discussed at the beginning of this section. |

# Service: Active Directory Replication

**Goal:** to ensure that replication between the hub (root domain) and spokes (agency bridgehead servers) occurs in a regular, timely manner.

## Replication Occurrence

It is the responsibility DIS to ensure that all the agencies that have signed service level agreements are included in the replication schedule and receive timely updates to their global catalogs. Replication will be scheduled by DIS and the individual agencies to occur at specific times.

Replication status will be verified on a daily basis using the following tools included with Windows 2000 and the Windows 2000 Resource Kit.

1. **Replmon.exe** – a graphical tool that you can use to view low-level status and performance of replication between Active Directory domain controllers.

2. **Repadmin.exe –** a command-line tool that lets you view and change replication status on domain controllers when you need to diagnose and troubleshoot replication between Windows 2000–based domain controllers. You can use Repadmin to view the current replication topology, manually create the replication topology, and force replication events.
3. **Event Viewer –** the windows 2000 event viewer should be monitored regularly to ensure that replication errors have not been recorded.  Any issues should be followed-up by DIS.

### Replication Verification

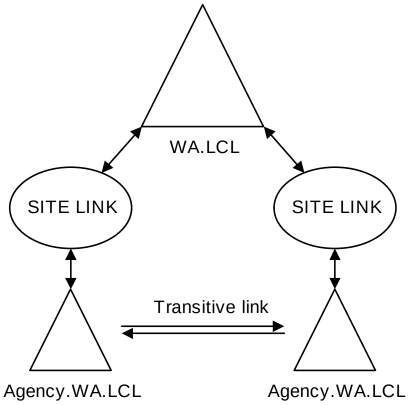
**Objective:** Verify that Active Directory Replication is occurring between the root domain controllers and all participating agencies.

To achieve this objective, root administrators must verify on a daily basis the following.

1. Replication failures between specific replication partners.

2. Both direct and transitive replication is occurring (agency changes are being reflected in other agency global catalogs).
3. FSMO roles at the forest and domain levels are consistent with the prescribed roles in the root requirements document.
4. Notice any changes to the replication topology that may have been initiated by agency administrators.
5. Monitor the count of failed replication attempts. Excessive failures that have not auto-corrected should be investigated (the level at which failed attempts becomes excessive will be defined by the replication schedule).

The replication topology of the State of Washington forest is consistent with the domain topology (each agency is its own site and domain, in spite of actual connection speeds between bridgehead servers).

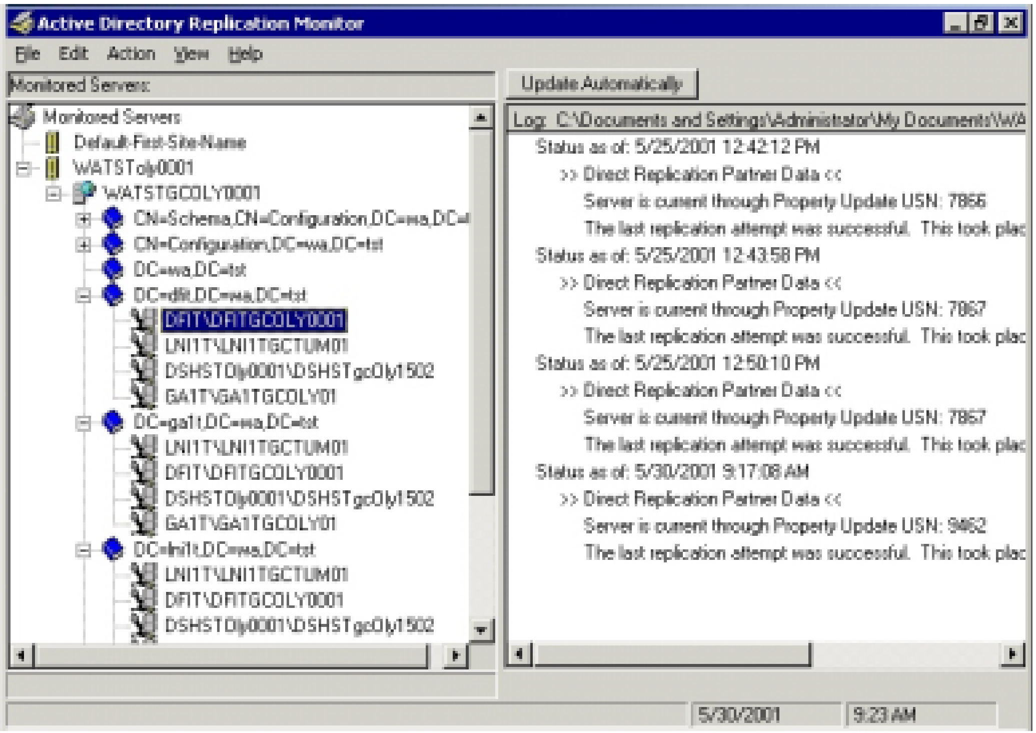


To properly achieve this objective, use the ReplMon.exe tool, found in the Windows 2000 Support tools, to monitor replication health.

| To Verify Replication Using Replmon.exe | |
|---|---|
| **Start Replmon and add monitored server.** | 1. From the start menu of the root domain controller, select Run and type ReplMon.exe at the command prompt. |

| | |
|---|---|
| | 2. Add the root domain controllers to the monitored servers list by selecting “Add Monitored Server” from the Edit menu.<br>3. Select the option “Add Server By Name” and enter WAgcOly0001 and WAgcLcy0001. |
| **Verify the status of servers.** | 4. Expand the DC containers for each of the Sub-sites to show replication partners within each site.<br>5. Look specifically for error icons for each of the domain controllers and their respective partners.<br>6. Use the information in the right-hand pane to investigate problems. |
| **Or use the web site to monitor domain health (available only on** | 1. Open the browser and point to http://watstgcoly0001.wa.tst/health.<br>2. You will be prompted for a user ID and password, specify an account with root |

| | |
|---|---|
| **test).** | domain administrator privileges.<br>3. On the left pane, select the sites link to bring up all active sites.<br>4. Drill down on the specific site by clicking the name in the site column. This will present you with a list of domain controllers in that site.<br>5. Click the name in the server column to return replication status with all server partners. |


Active Directory Replication Monitor
File Edit Action View Help
Monitored Servers:
Update Automatically

```
Monitored Servers
  Default-First-Site-Name
  WATSToly0001
    WATSTGCOLY0001
      CN=Schema,CN=Configuration,DC=wa,DC=t
      CN=Configuration,DC=wa,DC=tst
      DC=wa,DC=tst
      DC=dfit,DC=wa,DC=tst
        DFIT\DFITGCOLY0001
        LNI1T\LNI1TGCTUM01
        DSHSTOly0001\DSHSTgcOly1502
        GA1T\GA1TGCOLY01
      DC=ga1t,DC=wa,DC=tst
        LNI1T\LNI1TGCTUM01
        DFIT\DFITGCOLY0001
        DSHSTOly0001\DSHSTgcOly1502
        GA1T\GA1TGCOLY01
      DC=lni1t,DC=wa,DC=tst
        LNI1T\LNI1TGCTUM01
        DFIT\DFITGCOLY0001
        DSHSTOly0001\DSHSTgcOly1502
```

```
Log: C:\Documents and Settings\Administrator\My Documents\WA
  Status as of: 5/25/2001 12:42:12 PM
     >> Direct Replication Partner Data <<
        Server is current through Property Update USN: 7866
        The last replication attempt was successful.  This took plac
  Status as of: 5/25/2001 12:43:58 PM
     >> Direct Replication Partner Data <<
        Server is current through Property Update USN: 7867
        The last replication attempt was successful.  This took plac
  Status as of: 5/25/2001 12:50:10 PM
     >> Direct Replication Partner Data <<
        Server is current through Property Update USN: 7867
        The last replication attempt was successful.  This took plac
  Status as of: 5/30/2001 9:17:08 AM
     >> Direct Replication Partner Data <<
        Server is current through Property Update USN: 9462
        The last replication attempt was successful.  This took plac
```

## Replication Error Detection

Active Directory Sites and Services is the primary administrative tool that is used to manage replication. Use this tool to create connection objects and site links that the implement replication. Replication within a site is completely automatic and usually requires no intervention. Replication between sites is managed most effectively by changing the settings on the site link objects, as done in the State of Washington spoke and hub topology.

Communication from the KCC to the administrator occurs through event logs that you can view in Event Viewer. The following examples contain a few of the events that are generated by the KCC in the event log:

- Event 1009 (informational): The consistency checker has started updating the replication topology for this server.
- Event 1013 (informational): The replication topology update task terminated normally.

- Event 1265 (warning): The attempt to establish a replication link with parameters <parameters> failed with the following status: <error message>. The record data is the status code. This operation is going to be re-tried.
- Event 1311: The Directory Service consistency checker has determined that either (a) there is not enough physical connectivity published via the Active Directory Sites and Services Manager to create a spanning tree connecting all the sites containing the partition DC=mycorp,DC=com, or (b) replication cannot be performed with one or more critical servers in order for changes to propagate across all sites (most often due to the servers being unreachable).
- Event 1580 (Informational): A long running inbound replication has finished. The elapsed time was %1 minutes.
- Event 1540 (Warning): Due to contention with the Security Descriptor Propagator for resources, inbound replication was stalled for %1 minutes, %2 seconds. This condition

should be transient. If this issue persists, please contact Microsoft Product Support Services for assistance.

The KCC, like all subsystems in Active Directory, has a variable event logging level. By default, only the most important events are logged. You can increase the level of detail in the event log by modifying the value in the Replication Events entry in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics in the registry. Increasing the level of detail can be used to better understand the behavior of the KCC in different situations. However, a logging level value of greater than 2 generally results in excessive logging that degrades the performance of the component.

The Windows Event log should be checked on a daily basis for the above events.  Any instances of Event 1265 should be promptly investigated.

## Replication Performance

**Objective:** to ensure that proper hardware and network resources exist to allow Active Directory replication to occur in a timely manner.

### Establishing a Replication Baseline

To accomplish the performance objective for Replication Services, it is necessary to establish a baseline of metrics for total bytes replicated. This information will be captured using the Performance monitor tool in Windows 2000 and should be captured during "normal activity" over a period of 7 days. It should be recorded in 1 minute intervals 24 hours per day. The baseline will need to be re-evaluated for each significant change to the environment (new agencies, etc.). The following counters will be used.

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| NTDS | DRA INBOUND BYTES TOTAL | Total number of bytes replicated in. Sum of the number of uncompressed bytes (never |

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| | | compressed) and the number of compressed bytes (after compression). |
| NTDS | DRA OUTBOUND BYTES TOTAL | Total number of bytes replicated out. Sum of the number of uncompressed bytes (never compressed) and the number of compressed bytes (after compression). |

As you monitor the values of these counters, you might see occasional spikes. Typically, you can exclude these from your baseline because it is the consistent, repetitive values with which you are most concerned; the range of values that seem to appear consistently constitutes your baseline. When values fall outside of these ranges for extended periods, server activity should be investigated.

When trouble is suspected, the same performance monitor counters can be viewed real time and compare against the established baseline metrics.

| **To set up a baseline for Replication** | |
|---|---|
| **Create a new log using Windows 2000 Performance tools.** | 1. Open the Performance Application from the Administrative Tools Folder on the Start menu.<br>2. Expand performance logs and alerts.<br>3. Right-click counter logs and select New Log Settings.<br>4. Give the new log a name, describing the type of counters and period (e.g.: Replication Baseline May 2001). |
| **Specify counters, intervals, and file locations.** | 5. In the General Tab, click the add button to add the counters listed in the above table.<br>6. Set the sampling rate to every five minutes.<br>7. Switch to the Log Files Tab. |

| | |
|---|---|
| | 8. Specify a location on the D drive where the log files are to be archived (D:\performanceLogs\).<br>9. Ensure that file names end with the nnnnn format (this keeps an identity value that makes troubleshooting easier).<br>10. Switch to the Schedule tab.  Specify that start date as 12:00 PM (noon) for the next available Monday.<br>11. Specify the stop log for 12:00 PM (noon) exactly one week later.<br>12. Click Ok to save and schedule the performance log. |

## File Replication Service

Microsoft Windows 2000 Server uses the File Replication service (FRS) to replicate system policies and logon scripts stored in System Volume (SYSVOL). Each domain controller keeps a copy of SYSVOL for network clients to access. FRS can copy and maintain shared files and folders on multiple servers simultaneously. When changes occur, content is synchronized immediately within sites and by schedule between sites.

FRS performance is monitored using the Windows 2000 Event Viewer and Performance Counters of the FRS object.

Baseline performance metrics are already being captured on the NTDS objects during active directory replication. The FileReplicaSet object provides more granular counters, specific to the File Replication Service. DIS will consider use of these counters for troubleshooting purposes only. The recommended counters to watch during these times are listed below.

| OBJECT | COUNTER | DESCRIPTION |
|---|---|---|
| FileReplicaSet | Change Orders Received | Number of change notifications received from inbound partners. |
| FileReplicaSet | Change Orders Sent | Number of change notifications sent out to outbound partners. |
| FileReplicaSet | File Installed | Number of replicated files installed locally. |
| FileReplicaSet | KB of Staging Space Free | Amount of free space in the staging directory used by FRS to temporarily store files before they are replicated. The default staging space is 660 megabytes (MB). |
| FileReplicaSet | KB of Staging Space In Use | Amount of space in the staging directory currently in use. If the staging directory runs out of space, replication stops. |
| FileReplicaSet | Packets Received | Amount of data received locally. These packets can be change notifications, file data, or other command packets. |
| FileReplicaSet | Packets Sent | Similar to packets received. |
| FileReplicaSet | USN Records Accepted | Number of records that are accepted for replication. Replication is triggered by entries written to the NTFS change journal. FRS reads each file close record from the journal and determines whether to replicate the file. An accepted record |

| | | |
|---|---|---|
| | | generates a change order, which is then sent out. A high value on this counter (about one every five seconds) indicates a lot of replication traffic. |

### Checking the Event Log for FRS Objects

Check File Replication Service Event Log for inconsistency errors on a daily basis. Depending on the problems discovered, it may be necessary to perform a more detailed review the NTFRS related logs in %Systemroot%\Debug\ntfrs_0000x.log. The following table provides a list of events that could indicate a problem.

| NBR | EVENT LOG | DESCRIPTION |
|---|---|---|
| 13522 | File Replication Service | The File Replication Service is unable to add this computer to the following replica set: "DOMAIN SYSTEM VOLUME (SYSVOL SHARE)" |

| | | |
|---|---|---|
| 13555 | File Replication Service | The File Replication Service is in an error state. Files will not replicate to or from one or all of the replica sets on his computer until the following recovery steps are performed:<br>NOTE: Some Event ID descriptions have been truncated for brevity. |
| 1000 | File Replication Service | The Group Policy client-side extension Security was passed flags (17) and returned a failure status code of (3). |
| 1001 | File Replication Service | Security policy cannot be propagated. Cannot access the template. Error code = 3. |

# Service: Active Directory Database

**Goal:** to ensure that adequate resources are available in the Active Directory environment to properly manage the active directory database files and database performance.

## Database Performance

**Objective:** Ensuring the AD database is performing adequately and has the necessary hardware to support operations.

The Database object relates to the Extensible Storage Engine (ESENT), the transacted database system that stores all Active Directory objects. This performance object is not installed by default. The counters on the Database object enable you to perform advanced tuning of Active Directory. You can also use some of the counters to help determine whether you need more disk drives for storage of logs or database.

Currently, there is no automated way to install the performance dynamic-link library (DLL), Esentprf.dll, in Windows 2000.

### Establishing a AD Database Baseline

DIS will not actively monitor database performance counters unless part of a performance investigation. In order to expose the object counters, it is necessary to complete the following manual operation.

| **To Install Counters for the AD Database Object** | |
|---|---|
| | 1. Copy the performance DLL (Esentprf.dll) located in SystemRoot\System32 to any directory (for example, C:\Perf). |
| **Edit the Registry to allow Windows 2000 to see performance counter objects.** | 2. Run Regedt32.exe or Regedit.exe, and make sure that the following registry subkeys exist:<br>3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ESENT |

| | |
|---|---|
| | 4. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ESENT\Performance<br>5. If these subkeys do not exist, you need to create them.<br>6. For more information about creating registry subkeys, see Windows 2000 Server Help.<br>7. Make sure that, under the Performance subkey, the registry values that have the following settings exist:<br>a. Open : data type REG_SZ : OpenPerformanceData<br>b. Collect : data type REG_SZ : CollectPerformanceData<br>c. Close : data type REG_SZ : ClosePerformanceData<br>d. Library : data type REG_SZ : c:\perf\esentprf.dll |

| | |
|---|---|
| **Active the new counters.** | 8. Change directory to SystemRoot\Winnt\System32 or to another folder that contains the files Esentperf.ini and Esentperf.hxx generated when Eseperfnt.dll was compiled.<br>9. (Optional) To verify that previous counter information is not present in the registry, at the command prompt, type unlodctr.exe ESENT.<br>10. To load the counter information into the registry, run Lodctr.exe Esentperf.ini. |

Once the counters are activated, you should have access to the following performance measurements.

| Object | Counter | Description |
|---|---|---|

| Object | Counter | Description |
|---|---|---|
| Database | Cache % Hit | Indicates the percentage of page requests for the database file that were fulfilled by the database cache without causing a file operation. |
| Database | Cache Page Fault Stalls/sec | Indicates the number of page faults (per second) that cannot be serviced because there are no pages available for allocation from the database cache. |
| Database | Cache Page Faults/sec | Indicates the number of page requests (per second) for the database file that require the database cache manager to allocate a new page from the database cache. |
| Database | File Operations Pending | Indicates the number of reads and writes issued by the database cache manager to the database file or files that the operating system is currently processing. |
| Database | File Operations/sec | Indicates the number of reads and writes (per second) issued by the database cache manager to the database file or files. |
| Database | Log Record Stalls/sec | Indicates the number of instances (per second) that a log record cannot be added to the log buffers because the buffers are full. |
| Database | Log Threads Waiting | Indicates the number of threads waiting for data to be written to the log so that an update of the database can be completed. |
| Database | Table Open Cache Hits/sec | Indicates the number of database tables opened (per second) by using cached schema information. |

## Database Integrity

**Objective:** Ensure that the Active Directory database is up-to-date and that no consistency problems have been encountered during replication.

Because Active Directory is implemented on a transacted database system, the ESE historically called Jet, log files are used to support rollback semantics to ensure that transactions are committed to the database.

The Ntdsutil tool includes a semantics checker that can be invoked by selecting the Semantic database analysis option. The role of the semantic checker is to check the integrity of the contents of the Active Directory database.

The tool is run during Directory Service Restore mode. Errors are written into dsdit.dmp .xx log files. A progress indicator indicates the status of the check.

The following are examples of the functions that can be performed:

1. Reference count check. Counts all of the references from the data table and the link table to ensure they match the listed counts for the record. (For more information about data and link tables, see "Active Directory Data Storage" in this book.) It also ensures that each object has a GUID, distinguished name and nonzero reference count. If it is a deleted object, it ensures that it has a deleted time and date, but does not have a GUID or a distinguished name.
2. Deleted object check. Ensures that it has a deleted time and date, and a special relative distinguished name.
3. Ancestor check. Checks to determine if the current Distinguished Name Tag (DNT) is equal to the ancestor list of the parent and the current DNT.
4. Security descriptor check. Checks for a valid descriptor, ensuring that it has a control field, and that the discretionary access control list is not empty. If there are

deleted objects without a discretionary control access list, a warning is printed.

5. Replication check. Checks the UpToDate vector in the directory partition head to ensure that the correct number of cursors exist. It also checks to see that every object has “property metadata vector,” which is a global catalog attribute used for replication. For the instance type of the object, it checks the metadata, the up-to-dateness vectors, the sub references, and partial attribute.

| **To Perform Semantic Database Analysis** | |
|---|---|
| **This procedure should be performed monthly or whenever problems are suspected.** | 1. Back up Active Directory. Windows 2000 Backup natively supports backing up Active Directory while online. This occurs automatically when you select the option to back up everything on the computer in the Backup wizard, or independently by selecting to back up the "System State" in the wizard. |

| | |
|---|---|
| | 2. Restart the domain controller, select the appropriate installation from the startup menu, and press **F8** to display the **Windows 2000 Advanced Option Menu**.<br>3. Select **Directory Services Restore Mode**, and then press ENTER. To start the boot process again, press ENTER.<br>4. Log on by using the Administrator account with the password defined for the Local Administrator account in the offline SAM.<br>5. From the **Start** menu, point to **Programs** and **Accessories**, and then click **Command Prompt**.<br>6. At the command prompt, type **ntdsutil** and then press ENTER.<br>7. Type **Semantic database analysis**, and then press ENTER.<br>8. Type **Verbose on**, and then press ENTER. |

| | |
|---|---|
| | This displays the Semantic Checker.<br>9. Type **go,** and then press ENTER. The Semantic Checker is started without repairing any errors it encounters.<br>**Note:** To repair the errors encountered, select the **Go Fixup** option.<br>10. Type **quit**, and then press ENTER. To return to the command prompt, type **quit** again. |

# Security

**Goal:** to ensure that the fundamental security objectives of access control, availability and authentication are being met.

## Active Directory Backup

**Objective:** Ensure that information in Active Directory is backed up on a regular basis, providing the fastest possible recovery time and increasing availability of the active directory service.

Active Directory is backed up as part of System State, a collection of system components that depend on each other. These components must be backed up (and restored) together. Components that make up the System State on a domain controller include:

**System Start-up Files (boot files).** These are the files required for Windows 2000 to boot. They are automatically backed up as part of the System State.

**System registry.** The contents of the registry are automatically backed up when you back up System State data. In addition, a copy of your registry files are saved in the folder %SystemRoot%\Repair\Regback allowing you to restore the registry without doing a complete restore of the System State.

**Class registration database of COM+.** The Component Object Model (COM) is a binary standard for writing component software in a distributed systems environment. The Component Services Class Registration Database is backed up and restored with the System State data.

**SYSVOL.** The system volume provides a default Active Directory location for files that must be shared for common access throughout a domain. The SYSVOL folder on a domain controller contains the following:

1. Net Logon shares. (These usually host logon scripts and policy objects for non-Windows 2000–based network clients.)
2. File system junctions.

3. User logon scripts for Windows 2000 Professional–based clients and clients that are running Windows 95, Windows 98, or Windows NT 4.0.
4. Windows 2000 Group Policy.
5. File replication service (FRS) staging directories and files that are required to be available and synchronized between domain controllers.

**Active Directory.** This includes:

1. Ntds.dit. the Active Directory database.
2. Edb.chk. The checkpoint file.
3. Edb*.log. The transaction logs; each 10 MB in size.
4. Res1.log and Res2.log. Reserved transaction logs.
5. DNS Zone Data (backed up as part of the Active Directory Database)

## Best Practices for Backup

Back up an entire volume to prepare for the unlikely event of a disk failure. It is more efficient to restore the entire volume in one operation.

Always back up the directory services database on a domain controller to prevent the loss of user account and security information.

Always create and print a backup log for each backup. Keep a book of logs to make it easier to locate specific files. The backup log is helpful when restoring data; you can print it or read it from any text editor. Also, if the tape containing the backup set catalog is corrupted, the printed log can help you locate a file.

Keep three copies of the media. Keep at least one copy offsite in a properly controlled environment.

## Active Directory Backup Schedule

DIS will implement the following backup schedule.

1. Every night, the System State of all root domain controllers, as well as necessary ancillary files (log files, etc.) are backed-up to a single backup file server.
2. The backup file server is scheduled to be backed up within the same 24 hour period to the Tivoli Backup Silo. See the Root Domain Requirements document for more information about this process.
3. Once in the Tivoli system, files and their associated changes are preserved for 6 months. Any changes within that six month period are recoverable.

### Emergency Repair Disk

Emergency Repair Disk should be updated each time the system configuration changes, including updates to hardware, Service Packs, and applications that install services. As a safety measure, it’s recommended that administrators create an emergency repair disk on a weekly basis. Additionally, at least one, regularly updated copy of the ERD should be stored off-site.

### To create an Emergency Repair Disk

1. Open Backup.
2. On the Tools menu, click Create an Emergency Repair Disk.
3. The ERD Wizard will guide you through the process of creating the Emergency repair disk.

**Important**

You will need a blank 1.44 MB floppy disk to create an Emergency Repair Disk (ERD). The repair process relies on information that is saved in the %systemroot%\repair folder. You must not change or delete this folder.

## Hot Site Replication

**Objective:** ensure the availability of active directory services by verifying the Spokane domain controller is active, participating and available for recovery in the event of a disaster.

DIS currently maintains an active, participating domain controller in Spokane, Washington.  The DC is configured as a global catalog, but does not hold any of the FSMO roles.

The purpose of this server is two-fold.  First, it assumes standard operating functions of domain controllers and participates in the replication process between root and agency domains.  Second, it serves as a contingency server in the event of an Olympia disaster.

In the event of disaster, the Spokane domain controller may be responsible for seizing some or all of the FSMO roles from the Olympia environment.  The procedures for this are outlined in DIS' disaster recovery plan for Windows 2000.  As such, it is necessary to ensure that replication is occurring with the Spokane machine and that operations personnel in Spokane comply with the same performance monitoring and baselining activities that occur in Olympia.

## Authoritative Restore of Domain Controller

**Objective:** ensure data availability and integrity of active directory data to handle situations where directory information is corrupt or subject to other human error.

An authoritative restore is in essence an extension of the non-authoritative restore process. It requires all the steps of a non-authoritative restore before it can be initiated. The primary difference between the two is that an authoritative restore has the ability to increment the version number of the attributes of all objects in an entire directory, all objects in a subtree, or an individual object (provided that it is a leaf object) to make it authoritative in the directory.

As with a non-authoritative restore, once a DC is back online it will contact its replication partners to see what has changed since the time of the last backup. However, because the version number of the object attributes you wish to be authoritative will be higher than the existing instances of the attribute held on replication partners, the objects on the restored DC will appear to be more recent and therefore be replicated out to the rest of the DCs within the environment.

Unlike a non-authoritative restore, an authoritative restore requires the use of a separate tool (ntdsutil.exe) to make it work. No backup utilities—including the native Windows 2000 utility—can perform an authoritative restore.

An authoritative restore should be used when human error is involved such as when an administrator has accidentally deleted a number of objects; that change has replicated to all the DCs, existence of those objects is removed from the domain; and the administrator is unable to easily recreate these objects.

An authoritative restore will not overwrite new objects that have been created after the backup was taken. It can only be carried out on objects from the configuration and domain contexts. Authoritative restores of schema naming contexts are not supported.

The policies and procedures for performing an authoritative restore are documented in the Root domain requirements document and DIS' disaster recovery plan for Windows 2000.

### Authoritative Restores and Server Health

No health monitoring procedures are associated with an authoritative restore.  However, it is necessary to ensure that regular, versioned backups occur and are preserved for at least 12 weeks so that objects are available in the event they need restoration.

## Authentication and Access Controls

**Objective:** to ensure that only authorized personnel are performing administrative activity in the root domain and that security sensitive objects are controlled, audited, and access attempts logged.

| **To analyze Authentication and Access Controls** | |
|---|---|
| **Review Security Event Log Daily for failed logon attempts.  Report** | 1. For each domain controller, open the Event Viewer from the administrative tools folder in the start menu. |

| | |
|---|---|
| **any suspicious activity to root administration team.** | 2. Select Security Log<br>3. From the View menu, select Filter.<br>4. Clear all boxes except Failure Audit in the Event Types section.<br>5. Review records that were recorded in the previous 24 hours. |
| **Each week, save the security log to a file and clear out the log. This prevents the log from growing too large and preserves an audit trail. These logs should be kept for at least** | 1. Open Event Viewer.<br>2. From the Action Menu, select Save Log File As…<br>3. Choose a directory that is part of the nightly backup.<br>4. Use the following naming conventions for the file: "SecurityLogSSSMMMN.evt." SSS is the complete name of the server, MMM is a three character month name (e.g.: JAN), and N represents the week |

| | |
|---|---|
| **one year.** | of that month (e.g.: 1-5).<br>5. From the action menu, select Clear All Events. |

# Daily Operations Checklist

**Goal:** provide a checklist of operations functions that should be performed on a daily basis. The information provided here will reference other sections in the document.

**For Each Server In the Root Domain**

- □ Check Windows Event Log for DNS Errors (Page 45)
- □ Check Windows Event Log for Replication Errors (Page 58)
- □ Check Windows Event Log for File Replication Service Errors (Page 67)
- □ Verify that nightly backup completed without errors (Page 82)
- □ Verify the replication status using replmon or administrative web site (Page 52)

# Weekly Operations Checklist

**Goal:** provide a checklist of operations functions that should be performed on a weekly basis. The information provided here will reference other sections in the document.

### For Each Server in the Root Domain

- □ Verify that nightly backup completed without errors (Page 82)

□

# Monthly Operations Checklist

**Goal:** provide a checklist of operations functions that should be performed on a monthly basis.  The information provided here will reference other sections in the document.

### For Each Server in the Root Domain

□ Update, as necessary, changes to the Server Build Document and Standard Hardware Configuration (Page 11)

□ Schedule and configure settings for a processor utilization baseline update (Page 18)

□ Schedule and configure settings for a memory usage baseline update (Page 24)

□ Evaluate the need for an offline AD database defragmentation (Page 34)

- □ Evaluate the Completeness of Resource Records in the Root Domain (Page 44)
- □ Evaluate, configure and schedule Replication performance baseline if any major changes have occurred in the last 30 days (page 61)
- □ Update the Emergency Repair Disk (Page 83)

### Security Tasks

- □ Perform a trial restoration from backup on a lab server outside the production or test environments (Page 79)

### Reporting

- □ Prepare or update the trend analysis document from all available baseline metrics for each of the major services. Publish this on the DIS Windows 2000 Active Directory home page for other network administrators to view.